COMO PADRÕES NA FORMULAÇÃO DE SENHAS PODEM INTERFERIR EM SEU NÍVEL DE SEGURANÇA?

Giselly Nascimento de Oliveira
Lídia da Silva Nascimento
Osmar Gouveia Santiago
Renata Bezerra da Silva
Rogério Matheus Brasilino Gomes da Silva

RESUMO

Atualmente, o uso de senhas garante a segurança nos meios digitais. Entretanto, nota-se que certos padrões na hora da formulação de senhas comprometem a sua segurança e, consequentemente, a de seus usuários. Dessa forma, foi realizado um estudo a partir de dados obtidos com estudantes de cursos técnicos a fim de compreender melhor o fenômeno. Assim, concluiu-se que esse fenômeno se trata da união de fatores como a falta de conhecimento sobre o tópico. Além disso, foi possível observar que tal fenômeno não está restrito a um certo grupo de pessoas, de forma que pessoas com formação técnica também são suscetíveis a cometer tais erros.

Palavras-Chave: Senha; Privacidade; Padrões.

1. INTRODUÇÃO

Em um mundo cada vez mais integrado com a tecnologia, a maneira com a qual dados e informações são guardados é fundamental para garantir seu funcionamento. O tópico tornou-se alvo de diversos debates entre indivíduos e organizações, fazendo com que uma grande atenção fosse voltada para estudos na área. Apesar da criação de métodos de autenticação biométricos e de multifatores, uma das maneiras mais comuns de realizar a proteção dos dados é a partir do uso de senhas.

De acordo com NIST (2017), uma palavra-passe é uma sequência de caracteres utilizada para autenticar a identidade de um utilizador ao aceder a uma aplicação ou sistema. Sua eficácia, contudo, está diretamente ligada com a sua estrutura, de forma com que o uso de certos padrões tornam mais prático o processo de acesso a informações por terceiros. Isso representa um grande problema à segurança dos usuários, encontrando-se em posição vulnerável quanto a ataques, quebrando assim o que ainda se trata do método mais comum de proteção de dados.

Dessa forma, pretende-se verificar a relação desses padrões com a eficácia das senhas. Para que seja possível o entendimento desse tópico, será analisada a visão dos usuários quanto a importância de suas senhas, buscando também observar os padrões comumente usados e observar sua eficácia a partir de diversos parâmetros, buscando entender a maneira com que as pessoas escolhem suas senhas afetam diretamente sua proteção.

A análise desses fatores trata-se de uma maneira de analisar não apenas padrões a serem evitados na hora de formular uma senha, mas também a percepção dos usuários quanto a sua proteção na rede. Em um mundo onde tudo gira em torno da troca de informações, manter seus dados seguros é algo crucial para que os usuários mantenham sua integridade na plataforma. Gehringer (2002, p. 369, tradução nossa) aponta que “As palavras-passe são a primeira linha de

defesa contra a intrusão."

Intenta-se entender como as senhas funcionam e como elas são quebradas. Inicialmente, serão analisados os métodos convencionais de autenticação, seguidos da maneira com que os mesmos podem ser quebrados. Após isso, haverá um aprofundamento no entendimento do conceito de entropia, buscando assim compreender melhor os parâmetros necessários para a formulação de uma palavra chave. Por fim, haverá o processo da metodologia, onde os resultados serão observados de forma a entender não só como esses fatores afetam a proteção dos usuários, como também se os mesmos têm noção de sua existência e relevância.

2. REFERENCIAL TEÓRICO

2.1 AUTENTICAÇÃO

A conexão que o mundo mantém com a tecnologia, há a necessidade de garantir a segurança dos dados e informações de seus usuários. Para realizar tal feito, precisa-se haver maneiras de verificar a identidade do próprio. A integridade de suas operações pode ser garantida a partir de *autenticadores*, onde esses permitem verificar a identidade dos usuários ao realizarem uma operação. Essa autenticação pode ser realizada de algumas formas, sendo elas algo que a pessoa *sabe*, *possui* ou algo que é *intrínseco* a ela (FFIEC, 2005).

Autenticadores que envolvem algo intrínseco ao usuário podem ser vistos, por exemplo, a partir do uso de biometria, utilizando de algo associado diretamente à pessoa que está tentando acessar a plataforma, de forma com que apenas ele tenha acesso a isso. De acordo com uma matéria da BBC News (2014), um meio de autenticação que vem se tornando bastante popular com a maior acessibilidade e evolução da tecnologia dos celulares é o uso de digitais.

Uma outra alternativa se trata de coisas que os usuários possuam. Um exemplo disso são as transações bancárias. Para que elas sejam realizadas, é necessário que os usuários tenham acesso a um cartão, onde a partir dele é confirmado que a identidade de quem está realizando a transação, garantindo assim a integridade da transferência.

Apesar de serem opções eficazes, sua aplicação se torna ainda mais efetiva quando ligada a outros métodos de autenticação. Algo que ambas as soluções anteriores possuem em comum é o seu uso sendo habitualmente associado a algo que o usuário sabe, sendo feito geralmente a partir do uso de palavras chaves.

2.2 SENHAS

O uso de palavras-chave, também chamadas de senhas, se trata até os dias de hoje do método mais comum para realizar a autenticação de usuários, utilizando de uma sequência de caracteres. Tendo em vista que se trata de uma sequência de caracteres, é possível calcular a quantidade de senhas possíveis com uma determinada quantidade de caracteres.

Para cada caractere adicionado, o número de possibilidades cresce exponencialmente. Ao criar um PIN com seis números, onde os possíveis algarismos encontram-se entre 0 e 9, para cada caractere adicionado, as possibilidades de senha se tornam dez vezes maiores, sendo esse 10 o número de possibilidades de algarismos a serem escolhidos. Partindo desse princípio, existem 1.000.000 de possibilidades de PINs numéricos com seis dígitos.

Esse cálculo também pode ser usado para senhas mais complexas. Considerando que haja os 95 caracteres imprimíveis em ASCII para serem escolhidos durante sua formulação,

uma palavra-chave com os mesmos seis caracteres passa a ter 735.091.890.625 de possibilidades.

Apesar de ser uma recomendação o uso de senhas mais longas, elas não necessariamente indicam que o nível de proteção esteja adequado. De acordo com Roccia (2021, p. 6), "senhas como 'q1w2e3r4t5'e 'P@ssword1' seriam consideradas fortes, mesmo sendo umas das mais comuns. Portanto, apenas essas dicas não são suficientes." Isso se deve aos inúmeros métodos utilizados no processo de quebra de senha, onde são utilizadas verificações de padrões comuns na hora de sua formulação.

2.3 QUEBRA DE SENHAS

Um dos tipos de ataques mais convencionais é o ataque de força bruta. A definição dada por Silva, Heiderscheidt e Uriarte (2022) é de que se trata de um método em que há o esgotamento das senhas disponíveis, utilizando do poder de processamento para tentar todas as possibilidades possíveis.

Entretanto, o poder de processamento necessário e o tempo necessário torna o método inviável para senhas maiores, onde as possibilidades de senhas aumentam exponencialmente com o número de caracteres. Ainda de acordo com Silva, Heiderscheidt e Uriarte (2022, p. 8), "Um dos principais pontos que dificultam o ataque de força bruta são as diversas possibilidades de símbolos que podem ser inseridos nas senhas."

2.4 ENTROPIA

De acordo com Shannon (1948), conceitua-se como entropia a incerteza de possibilidades de uma variável aleatória. No meio da teoria da informação, ela é utilizada como forma de realizar a medição do nível de segurança de uma senha, levando em consideração o fator da randomicidade. Ela é medida a partir de *bits* e pode ser calculada com a seguinte fórmula:

$$H = log_2(b^1)$$

Existem duas maneiras de se calcular bits a depender de como as senhas foram geradas. No caso de ter sido gerada aleatoriamente, sua entropia pode ser calculada a partir do primeiro método. Entretanto, caso ela tenha sido escolhida pelo usuário, seu cálculo também leva em consideração fatores como o uso de letras maiúsculas, caracteres especiais e também o seu tamanho (NIST, 2017). A pesquisa de Silva, Heiderscheidt e Uriarte (2022) mostra que para que uma senha seja considerada segura, sua medição deve exceder o valor de 75 bits.

Nota-se, entretanto, que a evolução tecnológica das últimas décadas fez com que a entropia por si só não seja mais um método eficaz para a métrica de uma senha. Roccia (2021) aponta que nos últimos anos vem crescendo o uso de dicionários para a quebra de senhas.

2.5 DICIONÁRIO

Outros métodos surgiram e evoluíram ao longo dos anos. Modelos atuais utilizam do que é conhecido como *dicionário*. Nele, ao invés de tentar esgotar o limite de senhas disponíveis, o programa utiliza de padrões comuns de senhas entre os usuários, dados esses que geralmente são obtidos a partir do vazamento de senhas (Roccia, 2021).

Assim, mesmo ao cumprir requisitos básicos na hora de criar uma senha, a mesma não

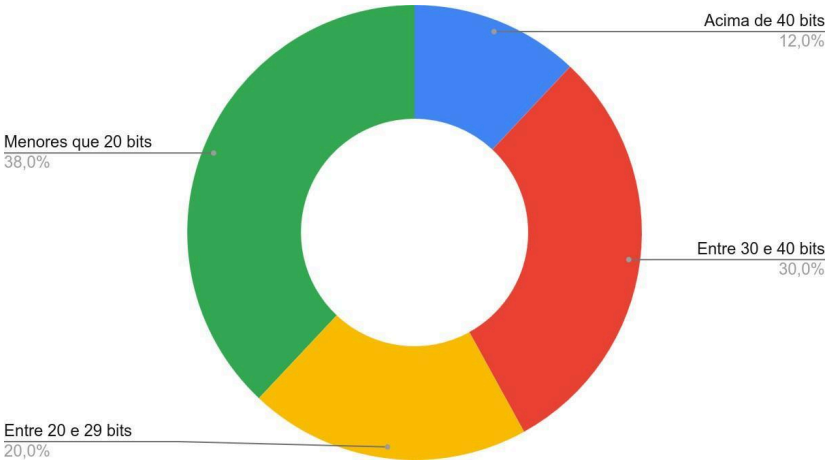
será efetiva caso siga certos padrões na hora de sua formulação, onde esses podem ser facilmente quebrados por programas do tipo. Uma pesquisa realizada por Silva, Heiderscheidt e Uriarte (2022), por exemplo, aponta que a senha "Henrique", que levaria 18 dias para ser quebrada usando força bruta, consegue ser quebrada em apenas 1 segundo.

2.6 VAZAMENTO DE SENHAS

O meio mais comum para a obtenção de dados para dicionários é a partir de vazamentos de senhas. com eles, é possível encontrar padrões comumente usados pelos usuários, facilitando o processo de quebra e, consequentemente, o acesso.

Uma matéria realizada pelo G1 (2021) aponta que a senha "123456" se trata até hoje da mais comum em vazamentos. Ela também aponta que apenas 12% das senhas encontradas no vazamento possuíam uma entropia acima de 40 bits, enquanto 38% delas tinham uma entropia menor que 20.

Figura 1 - Relação entre a entropia e a predominância de vazamentos



Fonte: Elaborada pelos autores (2025)

3. METODOLOGIA

De forma a garantir que a elaboração do estudo fosse fundamentada, foi adotada a pesquisa de campo como meio de obtenção de informações, buscando compreender diferentes perspectivas quanto a elaboração de senhas e suas possíveis consequências, analisando as informações obtidas a partir do referencial teórico, servindo como base para uma pesquisa qualitativa. O trabalho foi primeiramente elaborado a partir de um estudo de campo, que segundo Gonsalves (2001, p.67)

> A pesquisa de campo é o tipo de pesquisa que pretende buscar a informação diretamente com a população pesquisada. Ela exige do pesquisador um encontro mais direto. Nesse caso, o pesquisador precisa ir ao espaço onde o fenômeno ocorre, ou ocorreu e reunir um conjunto de informações a serem documentadas [...].

Primeiramente, foi realizado um estudo de caso tendo como base a aplicação de um questionário online. A partir dos dados apurados, foi-se observado o conhecimento dos

entrevistados sobre a elaboração de senhas e sua importância, além da segurança digital e a adoção de práticas que auxiliem em sua proteção.

A partir dos dados encontrados, foi realizada a sua análise a partir do referencial teórico. Buscou-se artigos dos mais diversos ramos da segurança digital. Dentre eles, encontram-se os trabalhos de Rubens Douglas, Joe Kissel, Edward F. Gehringer, Brandt Heiderscheidt, Ricardo Uriarte, Silveira da Silva, entre outros pesquisadores que se dedicaram ao estudo da segurança da informação. Assim, foi possível realizar a triagem dos dados obtidos.

4. RESULTADOS

Na pesquisa realizada, observou-se que **59,6% dos participantes** afirmaram possuir **quatro ou mais contas digitais**, o que indica uma alta demanda por gestão de senhas. Quando questionados sobre o uso de **gerenciadores de senha**, **61,4%** responderam que utilizam esse recurso, além de **78,9%** afirmaram utilizar **autenticação em dois fatores (2FA)** como medida adicional de segurança. Em relação à percepção de **segurança das próprias senhas**, **52,6%** dos respondentes disseram sentir-se seguros. No entanto, **63,2% dos participantes admitiram reutilizar a mesma senha em diferentes contas**.

Os dados obtidos, demonstram que embora a maioria dos participantes tenha consciência sobre práticas de segurança digital, como a autenticação de dois fatores, ainda existem comportamentos comprometedores da eficácia dessas medidas. Isso é demonstrado através dos altos índices de reutilização de senhas (63,2%) , o que demonstra contradição com o conhecimento é aplicação. Essa prática reduz a segurança do usuário, pois caso haja vazamento de uma senha, diversas contas podem ser comprometidas nesse processo. Observa-se portanto que a segurança não corresponde à execução dela .

Os resultados corroboram com as análises realizadas por autores como Roccia (2021) e Silva, Heiderscheidt e Uriarte (2022), as quais destacam a persistência de padrões possíveis na formação de senhas, mesmo em usuários conscientes. O estudo demonstra que a maioria das senhas ainda seguem lógicas facilmente previsíveis por programas de ataque de dicionário, o que reduz sua entropia, e consequentemente, a sua resistência a ataques automatizados. Esses achados reforçam que a educação digital e o incentivo a práticas seguras devem, além de práticas genéricas sobre complexibilidade, e tamanhos das senhas, enfatizando assim as problemáticas geradas pelos vazamentos é a importância da aleatoriedade e da não repetição.

De forma geral, os resultados apontam que a segurança das senhas está mais relacionada ao comportamento e às escolhas dos usuários do que às ferramentas utilizadas. Ainda que recursos como autenticação multifatorial sejam amplamente adotadas, o uso de padrões previsíveis e a reutilização de senhas comprometem a eficiência desses métodos. Isso evidencia a necessidade de maior conscientização sobre o impacto dos padrões na formulação das senhas, bem como a importância de práticas complementares, como o uso de geradores automáticos de senhas e políticas educacionais voltadas à segurança da informação.

5. CONSIDERAÇÕES FINAIS

Foi possível analisar que mesmo entre as pessoas que admitem se sentir seguras com relação a suas senhas, ainda há a ocorrência de más práticas de segurança, o que se trata de um fato preocupante quando levado em consideração que esses apontam possuir diversas contas,

aumentando a chance de terem sua privacidade violada a partir da exploração de vulnerabilidades. Ademais, muitos desses padrões prejudiciais podem ser vistos por pessoas que admitem ter uma boa segurança digital. Isso reforça que a ignorância pelo tópico faz com que os usuários sejam mais suscetíveis a cometer essas práticas.

Tendo em vista a questão inicialmente abordada, nota-se que a tendência a seguir certos hábitos é algo causado, por muitas vezes, pela ignorância quanto a práticas de segurança. Além disso, essas práticas não são exclusivas apenas para aqueles que não possuem formação da área da tecnologia, visto que os alunos entrevistados seguem cursos que abrangem a área tecnológica. Dessa forma, encontra-se como possível solução a conscientização sobre a formulação de senhas, além da conscientização sobre boas práticas de segurança digital.

A elaboração de perguntas que refletissem o foco principal desta pesquisa, além da análise dos padrões que eram seguidos na hora da escolha da palavra-chave, foram algumas das adversidades enfrentadas durante a elaboração do presente artigo. Notou-se que não bastava somente analisar os padrões que eram seguidos, mas também buscar entender o que levavam a esses padrões, além de observar outras práticas de segurança dos usuários. Logo, seria possível entender melhor as causas e contribuir com a fundamentação de soluções.

6. REFERÊNCIAS

FFIEC Press Release - October 12, 2005. Disponível em: <https://www.ffiec.gov/press/pr101205.htm>.

G1 GLOBO. As senhas mais comuns em vazamentos de dados no Brasil em 2021. Disponível em: <https://g1.globo.com/tecnologia/noticia/2021/11/18/as-senhas-mais-comuns-em-vazamentos-de-dados-no-brasil-em-2021.ghtml>

GONSALVES, Elisa Pereira. Iniciação à pesquisa científica. Campinas: Alínea, 2001.

GRASSI, P. A.; GARCIA, M. E.; FENTON, J. L. Digital Identity Guidelines. NIST Special Publication 800-63-3, 22 jun. 2017.

GEHRINGER, E. F. Choosing passwords: security and human factors. IEEE 2002 International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology. Proceedings (Cat. No.02CH37293), 2020.

KISSELL, J. Take Control of Your Passwords, 4th Edition. [s.l.] alt concepts, 2023.

KLEINMAN, Z. Politician's fingerprint "cloned from photos" by hacker. BBC News, 29 dez. 2014.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

ROCCIA, Rubens Douglas. Usuários respeitam as normas de criação de senhas seguras?: Uma análise de datasets de senhas vazadas. São Paulo, 2021 Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) - Universidade de São Paulo Instituto de Matemática

e Estatística. Disponível em: <https://bcc.ime.usp.br/tccs/2020/rubensd/Monografia.pdf>.

SHANNON, C. E. A Mathematical theory of communication. Bell System Technical Journal, v. 27, n. 3, p. 379–423, 1948.

SILVA, Eduardo Brandt Silveira da; HEIDERSCHEIDT, Henrique; URIARTE, Luiz Ricardo.**A influência da entropia das senhas na defesa contra ataques de força bruta**. *Revista de Extensão e Iniciação Científica da UNISOCIESC (REIS)*, v. 10, n. 1, 2022, ISSN 2358-4432. Disponível em: <https://dalfovo.com/ojs/index.php/reis/article/view/399/380>.

TRIVIÑOS, A. N. S. Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação. São Paulo: Atlas, 1987.

7. ANEXOS

ANEXO A - FORMULÁRIO

Como padrões na formulação de senhas podem interferir em seu nível de segurança?

Perguntas	**Respostas**
Quantas contas digitais você possui?	a) 1 b) 2 c) 3 d) 4 e) 5
Você utiliza gerenciadores de senha?	a) Sim b) Não
Sua conta possui autenticação de dois fatores?	a) Sim b) Não
Como você avaliaria o quanto se sente seguro com suas contas?	1 (Pouco seguro) 2 3 4 5 (Muito seguro)
Você usa a mesma senha em outras contas?	a) Sim b) Não
Escreva um exemplo de senha segura. Não use sua própria senha.	(Aberta)

8. FICHAMENTO

Citação	**Autor**	**Obra**	**Ano**

"Proposta originalmente no livro de Shannon (1948), A Mathematical Theory of Communication, a entropia na teoria da informação consiste na incerteza dos possíveis valores de uma variável randômica." (p.5)	ROCCIA, Rubens Douglas	Usuários respeitam as normas de criação de senhas seguras? Uma análise de datasets de senhas vazadas	2021
"No entanto, senhas como "q1w2e3r4t5" e "P@ssword1" seriam consideradas fortes, mesmo sendo umas das mais comuns." (p. 6)	ROCCIA, Rubens Douglas	Usuários respeitam as normas de criação de senhas seguras? Uma análise de datasets de senhas vazadas	2021
"Porém, isso é insuficiente nos tempos atuais, onde os programas de cracking de senhas como o John the Ripper utilizam ataques de dicionário, que levam em conta os padrões de criação de senhas comuns entre os usuários." (p. 6)	ROCCIA, Rubens Douglas	Usuários respeitam as normas de criação de senhas seguras? Uma análise de datasets de senhas vazadas	2021
"Diversos padrões de criação de senhas foram coletados pelo zxcvbn. Uma senha pode ter mais de um padrão de criação, como um nome e uma data de nascimento, por exemplo." (p. 10)	ROCCIA, Rubens Douglas	Usuários respeitam as normas de criação de senhas seguras? Uma análise de datasets de senhas vazadas	2021
"Os criptógrafos usam o termo entropia para se referir a uma aproximação matemática da complexidade de uma palavra-passe com base no método utilizado para a criar. Uma palavra-passe com maior entropia é mais difícil de adivinhar por uma pessoa (e, mais importante, por uma máquina)." (p.44)	KISSEL, Joe	Take Control of Your Passwords	2023
"Em vez disso, o software de cracking identifica padrões comuns de caracteres que poucos humanos notariam. Utiliza esta informação para testar as palavras-passe mais prováveis antes das menos prováveis, reduzindo o tempo médio necessário para obter uma correspondência. "	KISSEL, Joe	Take Control of Your Passwords	2023

"O ataque de força bruta consiste em esgotar as possibilidades de senhas, utilizando de poder de processamento para tentar todas as opções possíveis de todos os	Heiderscheidt , H., Brandt Silveira da Silva, E., & Ricardo Uriarte, L.	A Influência da Entropia das Senhas na Defesa Contra Ataques de Força Bruta	2022

caracteres, esse tipo de ataque demanda muito tempo e capacidade de equipamento." (p. 7)			
"Um dos principais pontos que dificultam o ataque de força bruta são as diversas possibilidades de símbolos que podem ser inseridos nas senhas." (p. 8)	Heiderscheidt , H., Brandt Silveira da Silva, E., & Ricardo Uriarte, L.	A Influência da Entropia das Senhas na Defesa Contra Ataques de Força Bruta	2022
"Através do presente trabalho, foi possível notar que a entropia de uma senha não pode ser um fator considerado por si só, já que mesmo tendo uma entropia alta a senha pode conter diversos padrões ou informações óbvias, inclusive que já foram vazadas e estão presentes em arquivos de vazamento disponíveis livremente na internet." (p. 10)	Heiderscheidt , H., Brandt Silveira da Silva, E., & Ricardo Uriarte, L.	A Influência da Entropia das Senhas na Defesa Contra Ataques de Força Bruta	2022
"Um dos principais pontos que dificultam o ataque de força bruta são as diversas possibilidades de símbolos que podem ser inseridos nas senhas" (p.8)	Heiderscheidt , H., Brandt Silveira da Silva, E., & Ricardo Uriarte, L.	A Influência da Entropia das Senhas na Defesa Contra Ataques de Força Bruta	2022
"As palavras-passe são a primeira linha de defesa contra a intrusão."	GEHRINGER, Edward F.	Choosing passwords: security and human factors	2002
"Embora seja óbvio que não se deve escolher uma palavra-passe que um intruso possa adivinhar facilmente, muitos utilizadores não apreciam a potência do arsenal que um hacker possui"	GEHRINGER, Edward F.	Choosing passwords: security and human factors	2002